International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Ingénierie des Systèmes d'Information
Vol. 29, No. 1, February, 2024, pp. 153-159
Journal homepage: http://iieta.org/journals/isi

# Algorithmic Framework for an Information System Ensuring Sustainable Development and National Security

Yulia Bobrova[1*], Yuriy Bobrov[2], Sergey Vavreniuk[3], Oleksandr Bondarenko[4]

[1] Department of International Law, Uzhgorod National University, Uzhgorod 88000, Ukraine
[2] Institute of Information, Security and Law, National Academy of Legal Sciences of Ukraine, Kyiv 01001, Ukraine
[3] Department of Fire and Technogenic Safety of Facilities and Technologies, National University of Civil Defense of Ukraine, Kharkiv 61108, Ukraine
[4] Department of Operational Art, National Academy of the National Guard of Ukraine, Kharkiv 61000, Ukraine

Corresponding Author Email: yuliia.bobrova@uzhnu.edu.ua

https://doi.org/10.18280/isi.290117

**Received:** 17 May 2023
**Revised:** 15 August 2023
**Accepted:** 25 August 2023
**Available online:** 27 February 2024

***Keywords:***
*sustainable development, information, security, system, information system, graphical modeling language*

## ABSTRACT

This study primarily aims to develop an algorithmic framework for constructing an information system dedicated to ensuring sustainable development and national security. The unique functionalities of this framework are manifested through the deployment of functional blocks, which, when represented with appropriate vectors and arrows, can facilitate superior organization and visualization of information. The scope of investigation is confined to the national information security system of a specific country. The primary scientific task undertaken in this study involves the modeling of an algorithm for constructing an information system that can ensure sustainable development and security. To accomplish this, the cutting-edge graphical modeling language of the Data Flow Diagram (DFD) standard is employed. The outcome of this study is a model that outlines the construction of an algorithm for the formation of an information system geared towards sustainable development and security. The novelty of this study lies in the methodological approach taken to develop the algorithm, which introduces a fresh perspective to addressing the issues at hand. The innovative aspect of this study is revealed in the modeled process of forming an information security system. However, the study is limited by the specific characteristics of the national security system of a single country. Future research in this domain should focus on modeling the integration of digital technologies into the national security system.

## 1. INTRODUCTION

### 1.1 The evolution of information systems: A critical review

As we traverse the current stage of human development, we stand at the cusp of a demographic explosion. The escalating demands of the burgeoning population outstrip even the pace of accelerated economic growth, leading to widespread impoverishment and resource depletion. In response, a new socio-economic development paradigm, "sustainable development", has emerged, which takes into account environmental limitations. This paradigm is grounded in an analysis of the causes of biosphere-wide environmental degradation and the exploration of strategies to mitigate threats to the environment and human health.

Over the past quarter-century, a global expansion of information networks has been observed, representing a unique confluence of computing and social communication. Within the context of sustainable development, the demand for mechanisms for information accumulation, systematization, storage, retrieval, transmission, and security is steadily increasing.

Scholars from the social sciences have proposed that we are entering the "information age", a new stage in human development characterized by the widespread use of information technologies that can transform the nature of social relations. This transformation has significant implications for national security systems, necessitating a reevaluation of challenges, threats, and state policies in this area, as well as the roles, functions, and responsibilities of security and defense forces within the framework of sustainable development.

### 1.2 The role of information systems in national security: An overview

In the era of information society, ensuring national security remains a challenge, further complicated by the increasing role of information. Information technology can provide stability and security, but it can also pose threats to these aspects. On one hand, information systems can facilitate the dissemination and exchange of security strategies, aid in peacekeeping missions, and implement and coordinate security plans and operations. They are integral to all government security operations, from intelligence gathering to command and control. On the other hand, information systems can also be exploited to undermine national security and stability.

Despite the theoretical and practical significance of the extant literature on the role of effective information systems in national security, a comprehensive academic exploration of the theoretical and legal foundations of national security in the information age is notably absent.

Therefore, the primary objective of this paper is to construct an algorithm for the formation of an information system that ensures sustainable development and security. To achieve this goal, the main scientific task is to model the construction of this algorithm, utilizing the contemporary graphical modeling language of the Data Flow Diagram (DFD) standard. The focus of the study is the national information security system. The structure of the paper includes a literature review, presentation of the main research findings, discussion, and conclusion.

## 2. LITERATURE REVIEW

As evidenced in recent scientific literature, information systems have ascended to a prominent position within the national security framework [1, 2]. In the contemporary global context, any nation's claim to supremacy in both military-technical and economic sectors, its strategic and tactical advantage, and its ability to successfully anticipate the emergence of new technologies, military equipment, and modern weapons, is contingent on its capacity to helm advanced media platforms and orchestrate an effective system of information conflict, including the ability to effectively counteract information warfare [3, 4].

Regrettably, a significant proportion of the extant literature investigating the role of information systems in national security lacks clear frameworks and mechanisms for the formation of these systems, thereby impeding their effective application in this domain.

The state's information policy, according to literary sources [5, 6], should address the pertinent issues that have arisen in international relations and information security. It is aptly emphasized that legislative protection of the rights and interests of all participants in information relations must be ensured [7, 8].

The literature also highlights that mechanisms for managing information security are lagging considerably behind the current level of informatization. This discrepancy contributes to the rise in cybercrime, leading to severe, and occasionally irreversible, consequences for states, enterprises, societies, and individuals [9, 10]. Researchers identify a broad spectrum of cybercrimes, encompassing crimes committed for financial gain and crimes related to the use of information stored in computers, tablets, and mobile phones, as well as crimes against the confidentiality, integrity, and availability of computer systems. Addressing the issues of combating cybercrime is recognized as a critical aspect of modern national security.

Despite the theoretical and practical significance of these and numerous other literary sources [11, 12], a comprehensive academic exploration of the theoretical and legal foundations of national security in the information age has not been undertaken. The shift in the nature of social interactions in the information age necessitates alterations in the corresponding regulators of these interactions, specifically, the methodological approach. This factor, the information system, which affects the nature of threats to national security, also requires the appropriate organization of countermeasures at the state level.

This highlights the necessity of addressing the scientific and theoretical problem of developing a conceptual approach to model the algorithm for the formation of an information system that ensures sustainable development and security. The primary scientific task, therefore, is to model this algorithm's construction.

## 3. METHODOLOGY

### 3.1 Description of the used methodology

The main method of constructing the algorithm will occur through the use of modeling methodology. In fact, it is necessary to create a unified language for structural analysis and design, suitable for modeling information systems, having the following characteristics: expressiveness, which allows considering the system from different positions - functional, informational, behavioral; ease of understanding and use; continuity within the modeling cycle - from models to models of the algorithm for the formation of an information system to ensure sustainable development.

The proposed solution is based on the DFD technology, which is the most complete in terms of possession of the listed characteristics among modern classical structural approaches (such as, for example, the integrated IDEF technology, including the IDEF0, IDEF1X, IDEF3 models or the so-called ARIS “methodology”). As an alternative approach to solving this problem, it is necessary to note studies based on ontological models of structural languages.

The reason for choosing this modeling methodology is that DFD is designed to model information systems that are directly related to our study.

### 3.2 Key parts of the chosen methodology

For further presentation of the material, it is necessary to recall that the classical DFD technology is based on three groups of modeling tools: diagrams illustrating the functions that the system must perform, and relationships between these functions - DFD (Data Flow Diagrams) data flow diagrams are used for this purpose, supplemented by data dictionaries and lower-level process specifications; diagrams that model data and their relationships - for this purpose, entity-relationship diagrams ERD (EntityRelationship Diagrams) are used; diagrams that model the behavior of the system - for this, state transition diagrams STD (State Transition Diagrams) are used.

The basis and connecting medium of the complex model is the DFD diagram, which demonstrates data recipients and destinations external to the system, identifies logical functions (processes) and groups of data elements that connect one function with another (streams), and also identifies data storage devices (storages), to which access is being made.

Also, as part of our study, it is necessary to conduct a SWOT analysis of the state of national security of a single country, for which the modeling of the construction of an algorithm for the formation of an information system will take place. The Czech Republic will be such a country. The reason for the choice is the residence of the team of authors in this country. The choice of the Czech Republic is due to the fact that recently the demand for information support for national security has increased in the Czech Republic, and in most regions of the country, the modernization of information systems has intensified as part of ensuring national security.

The use of SWOT analysis is envisaged before the simulation. The purpose of its use is to analyze the environment, identify weaknesses and threats in order to further use these results in modeling using DFD. There were two steps in the SWOT analysis system: direct SWOT analysis and evaluation of its results; using the findings and results of SWOT analysis in modeling using DFD.

## 4. RESULTS OF RESEARCH

### 4.1 The results of the SWOT analysis

Thus, we will conduct a SWOT analysis in order to clearly understand what kind of problems of ensuring sustainable development and security exist in the country in order to take into account when modeling the algorithm for forming an information system (Table 1).

The identified weaknesses and dangers were taken into account when constructing the method. In our opinion, in modeling, first of all, it is important to identify and highlight problems and weaknesses in order to subsequently take them into account in the modeling process.

**Table 1.** Matrix of SWOT analysis regarding the state of national security of the country in the framework of sustainable development

| S | W | O | T |
|---|---|---|---|
| Implementation of information changes | Lack of information cooperation | Digitalization of society | Unauthorized access |
| Modern equipment | Low information confrontation | Emergence of new technologies | Information leak |
| Development of digital infrastructure | Problems with information patronage | Creation of cyberpolice | Disclosure of security information |

### 4.2 The results of the modeling

Thus, the construction of any algorithm begins with a goal and processes for achieving it. In our case, we will designate such a goal as A - Formation of an information system for ensuring sustainable development and security (Figure 1).

The algorithm for the formation of an information system for ensuring sustainable development and security through modeling in the DFD language is shown in Figure 2.

Let us consider in detail each process of the algorithm in more detail:

1A. Formation of information patronage. Information patronage is a form of ensuring information security by the state of individuals and legal entities. Information security includes obtaining various information about destabilizing factors and information threats, the exchange of information between management bodies and information security system tools, Information protection is carried out in different ways, namely from the adoption of bills to the adoption of operational measures by information security forces in the process of intelligence, counterintelligence, operational-search and operational-information activities.

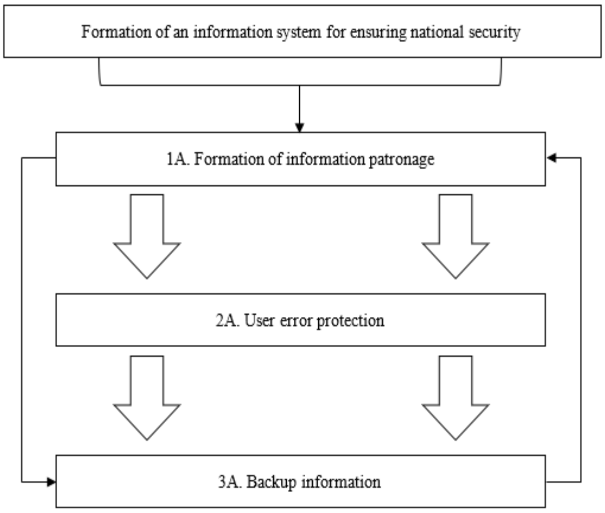
Formation of an information system for ensuring national security
1A. Formation of information patronage
2A. User error protection
3A. Backup information

**Figure 1.** Processes for achieving the goal of modeling

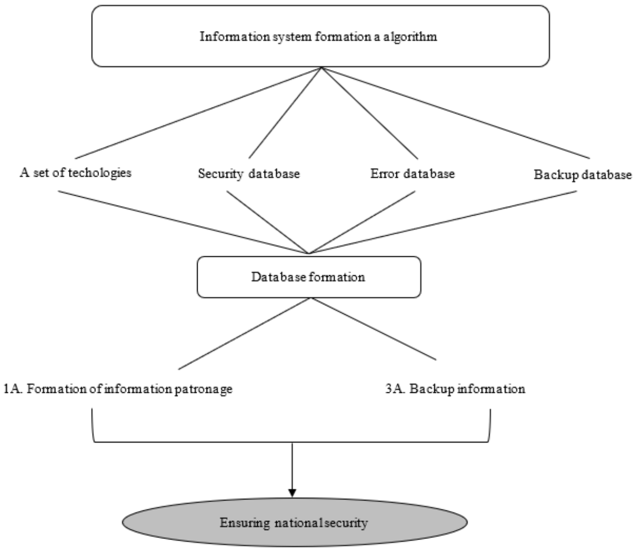

**Figure 2.** The algorithm for the formation of an information system for ensuring sustainable development and security through modeling in the DFD language

Process detail
Flexibility
Manufactu rability
Security and safety
Database

**Figure 3.** The main characteristics of the proposed model

2A. User error protection. For safe work in the local and global Internet information network, it is important to configure the security settings of the viewer program, as well as monitor the network activity of network computers in order to detect and block network threats in a timely manner. To protect against user errors when working with important documents, it is necessary to use the means of resolving individual documents and information directly in the document. This can be achieved using the features of office programs: templates and protection

3A. Backup information. It is important for the enterprise to back up important information and create copies of trimmed system disks of personal computers and servers at the time of their normal operation. The combination of these measures will allow the resumption of work in the shortest possible time. Restriction of rights to change system information, application of automated protection rules, scheduled updating and checking of systems, timely collection and analysis of information activity during user operation will protect against accidental errors in the operation of the information system. In many ways, the correct actions in these areas depend on the qualifications of the computer network administrator.

Among the main characteristics of the proposed model, the following can be distinguished, presented in Figure 3.

In addition to the main model, the main information functions of ensuring sustainable development and security through modeling should also be presented (Figure 4).

The main information functions of ensuring sustainable development and security through modeling by DFD technologies are shown in Figure 5.

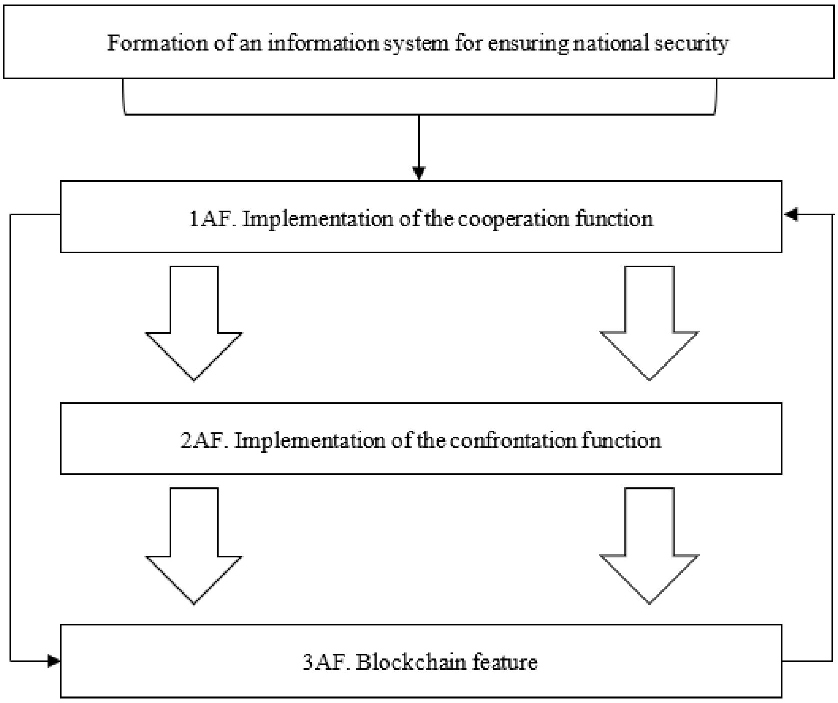
Formation of an information system for ensuring national security
1AF. Implementation of the cooperation function
2AF. Implementation of the confrontation function
3AF. Blockchain feature

**Figure 4.** The main functions of facilitating the construction of the algorithm

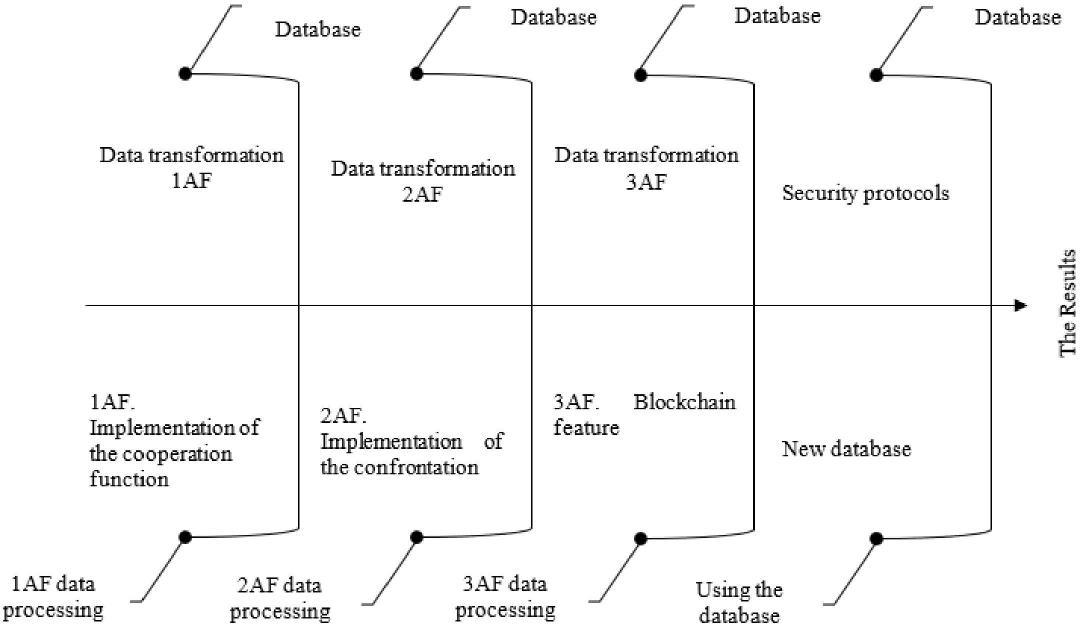

**Figure 5.** The main information functions of ensuring sustainable development and security through modeling by DFD technologies

Let us consider in detail each process of the algorithm functions in more detail:

1AF. Implementation of the cooperation function. Information cooperation is a form of ensuring information security between equal subjects of the information process, including a set of mutually agreed actions aimed at obtaining information about the destabilization of information security in the country, information threats and methods of dealing with them.

2AF. Implementation of the confrontation function. Information warfare is a form of competition between social systems in the information sphere in terms of influencing various spheres of social relations and establishing control over the sources of strategic resources, as a result of which one of the groups will receive the advantages they need for further development. Information confrontation occurs between different types of social subjects, but a whole series of such interactions form separate forms of confrontation (information wars, crime, terrorism).

3AF. Blockchain feature. Blockchain technology is inextricably linked with digital currencies, therefore, certain shifts are observed in this area, especially in terms of the adoption of cryptocurrency. Regardless of where and how blockchain is used, decentralization is a key factor in its use as an information security technology. When access control, network traffic, and even the data itself is no longer stored in one place, it becomes much more difficult for cybercriminals to attack information resources.

Thus, as a result, we have obtained an algorithm for the formation of an information system for ensuring sustainable development and security through the modeling method. In general, the key characteristics of this model show its positive aspects. The results of the study meet our expectations. The presented models are what we expected at the beginning of the study. In our opinion, the results are holistic and complex.

## 5. DISCUSSIONS

When discussing the results of our study, a comparison with similar ones should be made. So, Sylkin et al. [13, 14] noted that in the XXI century in the national security system, the information system occupies a leading place. For a long historical period, the information system was primarily associated exclusively with the interests of the state. The theory of information security has acquired a different content and has been transformed under the influence of the development of information and communication technologies. Currently, the information system within the country is spreading in the following areas: the state, society (or part of it, a group of people) and the individual. A separate fundamental area is international information security. Accordingly, the information system has a two-level meaning: 1) national; 2) international.

Stadelmann et al. [15, 16] came to the conclusion that information and communication technologies are one of the most important factors in stimulating economic growth and the development of civil society, employment, expanding competition, and, as a result, helping to overcome the "digital divide". The special role of the Internet in the life of the state and society opens up new opportunities for the formation of the socio-economic sector, personal development and other positive factors. But at the same time, threats of various levels arise (from electronic robbery of citizens to hacking of the state information system, which can affect the economy of the entire country), which cannot always be prevented or quickly resolved.

As a result, Kryshtanovych et al. came to the conclusion that until recently, the issue of protecting personal information did not arouse any interest on the part of citizens [17, 18], but in recent years it has been of unconditional interest, which is associated with various factors, such as the development of information and communication technologies; the desire to influence a person by illegally obtaining his personal information, etc. However, more negative consequences appear when such influence is exercised on civil servants, public authorities as a whole, since in this case the interests of a much larger group of people or, in general, the interests of the whole country (national interests) may be violated.

Kryshtanovych et al. came to the conclusion that the creation of a modern value system (information culture) and its integration into society will become the foundation for ensuring the information security of a person and the state [19, 20]. However, this approach is effective only within the state, since, as is known, threats also arise outside its territory. As a result, the information system includes two main areas: protection of information (both public and private) and protection from information (concerning mainly individuals or groups of persons). At present, the priority task of the state is to develop strategies and implement a unified state policy in this direction. Not only the development of individual areas, but also the level of democratization of society depends on an effective state information policy. The absence of a clearly formulated state information policy and the determination of the real possibilities of the state in this direction complicates the protection of the information interests of society and contributes to information attacks by internal and external aggressors.

Alazzam et al. [21-23] consider information systems through certain steps or proposals for the process of forming information systems. Our study is similar in that stepwiseness is important in the algorithm for building an information system. At the same time, the difference is that we offer a completely different methodological approach to building an algorithm for the formation of information systems, taking into account aspects of national security.

Discussing the results of our study, a number of innovative aspects should be noted. The scientific novelty of the obtained results lies in the fact that we used a new methodological approach to constructing an algorithm for the formation of an information system for ensuring sustainable development and security. This approach will systematize and simplify the process of forming information systems in the context of ensuring national security. The innovativeness of the article reveals the process of modeling the method of forming an information security system. The results obtained make it possible to build information systems in a new way, to provide and implement them. The applied modeling language contributes to better visualization and simplicity. The study is limited to taking into account the specifics of the national security system of only one country.

## 6. CONCLUSIONS

So, as a result, a model for constructing an algorithm for the formation of an information system for ensuring sustainable development and security was obtained.

Summing up, it should be noted that the policy of forming an information system should be focused on ensuring guarantees of information sovereignty and information security of all subjects in the field of informatization, since information support for national security is a process of meeting the information needs of subjects of national security in the framework of sustainable development.

Critical periods in the development of society are always associated with changes in socio-economic and demographic processes, which makes it necessary to revise traditional ideas about the organization of the environment and develop new principles and methods for managing the development of a new paradigm of social development. There have been many critical periods in the history of mankind, each of which generated an explosive wave of scientific creativity, which accelerated the development of society. Modern sustainable development can be defined as critical, which is caused by a global inconsistency between its economic, environmental and social components.

The study is limited by taking into account the specifics of the national security system of only one country. Prospects for further research should be devoted to modeling the integration of digital technologies into the national security system in the framework of sustainable development.

## REFERENCES

[1] Barrett, M.P. (2018). Framework for improving critical infrastructure cybersecurity version 1.1. Cybersecurity Framework. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.04162018

[2] Pan, L., Tomlinson, A. (2016). A systematic review of information security risk assessment. International Journal of Safety and Security Engineering, 9(2): 270-281. https://doi.org/10.2495/SAFE-V6-N2-270-281

[3] Alcántara, M., Melgar, A. (2016). Risk management in information security: A systematic review. Journal of Advances in Information Technology, 7(1): 1-7. https://doi.org/10.12720/jait.7.1.1-7

[4] Boiarynova, K., Popelo, O., Tulchynska, S., Gritsenko, S., Prikhno, I. (2022). Conceptual foundations of evaluation and forecasting of innovative development of regions. Periodica Polytechnica Social and Management Sciences, 30(2): 167-174. https://doi.org/10.3311/PPso.18530

[5] Fenz, S., Ekelhart, A. (2011). Verification, validation, and evaluation in information security risk management. IEEE Security & Privacy, 9(2): 58-65. https://doi.org/10.1109/MSP.2010.117

[6] Bialas, A. (2006). Information security systems vs. critical information infrastructure protection systems-Similarities and differences. In 2006 International Conference on Dependability of Computer Systems, pp. 60-67. https://doi.org/10.1109/DEPCOS-RELCOMEX.2006.30

[7] Kholiavko, N., Popova, L., Marych, M., Hanzhurenko, I., Koliadenko, S., Nitsenko, V. (2020). Comprehensive methodological approach to estimating the research component influence on the information economy development. Naukovyi Visnyk Natsionalnoho Hirnychoho Universytetu, 4: 192-199. https://doi.org/10.33271/nvngu/2020-4/192

[8] Paré, G., Trudel, M.C., Jaana, M., Kitsiou, S. (2015). Synthesizing information systems knowledge: A typology of literature reviews. Information & Management, 52(2): 183-199. https://doi.org/10.1016/j.im.2014.08.008

[9] Dzobelova, V.B., Ilaeva, Z.M., Melenchuk, A.S. (2020). Information security issues in the age of digital economics. In Proceedings of the First International Volga Region Conference on Economics, Humanities and Sports (FICEHS 2019), 114: 227-229. https://doi.org/10.2991/aebmr.k.200114.053

[10] Hrybinenko, O., Bulatova, O., Zakharova, O. (2020). Evaluation of demographic component of countries' economic security. Business, Management and Economics Engineering, 18(2): 307-330. https://doi.org/10.3846/jbem.2020.12309

[11] Kryshtanovych, M., Panfilova, T., Khomenko, A., Dziubenko, O., Lukashuk, L. (2023). Optimization of state regulation in the field of safety and security of business: A local approach. Business: Theory and Practice, 24(2), 613–621. https://doi.org/10.3846/btp.2023.19563

[12] Sylkin, O., Shtangret, A., Ogirko, O., Melnikov, A. (2018). Assessing the financial security of the engineering enterprises as preconditions of application of anti-crisis management: Practical aspect. Business and Economic Horizons, 14(4): 926-940. https://doi.org/10.15208/beh.2018.63

[13] Sylkin, O., Kryshtanovych, M., Zachepa, A., Bilous, S., Krasko, A. (2019). Modeling the process of applying anti-crisis management in the system of ensuring financial security of the enterprise. Business: Theory and Practice, 20: 446-455. https://doi.org/10.3846/btp.2019.41

[14] Yan, H.N. (2016). Research on the evolution path of the civil-military integration of innovation ability in national defense industry. Science & Technology & Economy, 29(2): 16-20. https://doi.org/10.3969/j.issn.1003-7691.2016.02.004

[15] Stadelmann, D., Portmann, M., Eichenberger, R. (2015). Military careers of politicians matter for national security policy. Journal of Economic Behavior & Organization, 116: 142-156. https://doi.org/10.1016/j.jebo.2015.04.001

[16] Ellefsen, I., von Solms, S. (2010). Critical information infrastructure protection in the developing world. In T. Moore & S. Shenoi (Eds.), Critical Infrastructure Protection IV. ICCIP 2010. IFIP Advances in Information and Communication Technology, Springer, 342: 25-36. https://doi.org/10.1007/978-3-642-16806-2_3

[17] Soomro, Z.A., Shah, M.H., Ahmed, J. (2016). Information security management needs more holistic approach: A literature review. International Journal of Information Management, 36(2): 215-225. https://doi.org/10.1016/j.ijinfomgt.2015.11.009

[18] Alazzam, F.A.F., Tubishat, B.M.A.R., Savchenko, O., Pitel, N., Diuk, O. (2023). Formation of an innovative model for the development of e-commerce as part of ensuring business economic security. Business: Theory and Practice, 24(2): 594–603. https://doi.org/10.3846/btp.2023.19781

[19] Kryshtanovych, M., Petrovskyi, P., Khomyshyn, I., Bezena, I., Serdechna, I. (2020). Peculiarities of

implementing governance in the system of social security. Business, Management and Education, 18(1): 142-156. https://doi.org/10.3846/bme.2020.12177

[20] Saleh, A.J., Alazzam, F.A.F., Rabbo Aldrou, K.K.A., Zavalna, Z. (2020). Legal aspects of the management of cryptocurrency assets in the national security system. Journal of Security & Sustainability Issues, 10(1): 235-247. https://doi.org/10.9770/jssi.2020.10.1(17)

[21] Alazzam, F.A.F., Salih, A.J., Amoush, M.A.M., Khasawneh, F.S.A. (2023). The nature of electronic contracts using blockchain technology – Currency Bitcoin as an example. Revista De Gestão Social E Ambiental, 17(5): e03330. https://doi.org/10.24857/rgsa.v17n5-014

[22] Al Azzam, F. (2019). The adequacy of the international cooperation means for combating cybercrime and ways to modernize it. JANUS.NET E-Journal of International Relations, 10(1): 75-98. https://doi.org/10.26619/1647-7251.10.1.5

[23] Bazyliuk, V., Shtangret, A., Sylkin, O., Bezpalko, I. (2019). Comparison of institutional dynamics of regional development publishing and printing activities in Ukraine: Methodological and practical aspects. Business: Theory and Practice, 20: 116-122. https://doi.org/10.3846/btp.2019.11